Published and Copyright (c) 1999 - 2007
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Patrice Mandin

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #0930 07/27/07

~ Anti-Phishing Research! ~ People Are Talking! ~ New SDL Release!
~ Eavesdropping On E-mail ~ Facebook Faces Charges ~ Online Feud, Arson!
~ Dell Expands Linux PCs! ~ Test Your Knowledge! ~ Feds Warn Public!

~ FBI, China Bust Pirates ~ DIY Trojan Tool On Web ~ Internet Tax Debate!

-* Young Keep High-Tech Simple! *-
-* OLPC Now Ready for Mass Production! *-
-* MySpace IDs & Deletes 29,000 Sex Offenders *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

First Britney, then Nicole, then Paris, Lindsay, Britney again, ad nauseum! What is it with the former Disney stars and their "born with a silver spoon in their mouth" friends? Send them all to/back to jail and keep them there for awhile. No, not a couple of weeks of isolation like Paris got. Put them in the general prison population - that might just scare them straight. What a bunch of spoiled, talent-less brats. They sound like troubled adolescents who really need some help. Instead of buying professional help to get them out of their jams, maybe they should seek some other professionals to make them understand themselves. You'd think that with all of their money, they would make something out of themselves besides scandalous headlines.

Hey, have you read the latest/final entry in the Harry Potter series? I'm down to the last chapter or two; I was told that I have to finish it by the end of the day so my wife can dive into it. Anyway, if the "rumor" is true, and this is indeed the last installment of the series, it will be too bad. Yes, I've read them all, and I'll miss the anticipation of another one. No more Hogwarts, nor wizards, nor Muggles. This is the end. Whether or not this is a "good" decision is open to debate. Ride out on a broomstick while still on top? Perhaps. It was a fun ride while it lasted.

Sounds a little like our ride with Atari, doesn't it. We kept hearing about the latest and greatest machines coming out, and we continued to crave that news - had to have each new model. But, similar to Harry Potter, the ride came to an end - and we knew that the "death knell" was coming. While Harry Potter climbed immediately to the forefront, Atari did not, except to its most dedicated fans. And even they realized that Atari couldn't maintain its [limited] stature.

But have faith Harry Potter fans. We can still read the series of books over and over again. We can discuss the merits of wizardry, or the history of the Hogwarts' ghosts. And just as possible, dedicated Atari fans can continue to enjoy their machines and use those terrific programs that we've come to know extremely well over the years. As long as we "keep the faith", both will always be there for us, one way or another.

And to tie this all into my Hollywood nymphets comments, maybe all four of them could use a good Transfiguration spell cast upon them!

Until next time...

=~=~=~=

SDL 1.2.12

Hello,

Here is a new SDL release, available on my web site:
- Teamtap support (4-joypad adaptors).
- Fixes in mouse and keyboard management.
- Save and restore FPU registers in audio and timer interrupts.
- GEM: allow creation of windows bigger than screen resolution.
- GEM: better mouse grab.
- And more fixes not specific to Atari version.

Thanks to Keith Scroggins for the intensive tests with Scummvm and Openttd :).

--
Patrice Mandin
WWW: http://pmandin.atari.org/
Programmeur Linux, Atari
SpØcialitØ: DØveloppement, jeux

=~=~=~=

PEOPLE ARE TALKING
compiled by Joe Mirando
joe@atarinews.org

Hidi ho friends and neighbors. Well, another week has come and gone, and there's (surprise!) another 'celebrity' scandal. Poor little Lindsay Lohan.

I'm guessing that Dana may want to say something about celebs and their 'problems', so I'll keep it real short on this subject.

Call me old fashioned or call me a hardass, but this chick is in desperate need of 18 months of wearing a smock and punching a cash register for minimum wage. And those who've 'enabled' her (gawd, I hate that word), well they would, of course, be entitled to their 10%.

Okay, enough of that. I was going to talk about politics, but I'll bet you're pretty tired of that. Then I thought about probing into why it seems that everyone has 'better' cell phone technology than the United States... but that's a lot of research and, quite honestly, I'm not up for that much work. Then I thought; how 'bout the success of the Harry Potter books and their author, J.K. Rowling?

We have a winner! Yeah, let's talk about Harry Potter. It's not that I think that these are the best-written books ever, or that their author

is a genius (although there's no doubt that she's very, very intelligent), but that she had the right idea at the right time and followed through on it. If she'd written half of the first chapter and said, "oh, the hell with it", who would have ever heard of Joanne Rowling?

She went from 'Welfare Mother' to 'Billionaire in the span of 15 years, and she did it the good old-fashioned way: She found something she loved and was good at, and she stuck with it.

And to those who complain about 'occult' subject matter and such I say, 'get a life'. If you're worried about Harry Potter turning your kids into baby-eating satanists, then sit them down and (gasp!) talk to them.

Besides, 'occult' doesn't necessarily mean 'bad'. It means 'pertaining to magic' or 'hidden'. By that definition, TRUTH is becoming occult. There's no baby-eating, no animal sacrifice, no Black Mass.

No, by far the lion's (or griffin's) share of this series of books deals with morality, personal responsibility and integrity.

Of course, those are dangerous traits. They all require independent thought and a willingness to break rules when necessary.

I can remember reading Adventures of Huckleberry Finn, when Huck ruminates about slavery. "Preacher don't say it's wrong", was the phrase that's always stuck in my mind (but to be honest, I don't remember the exact wording). Huck, like most of us, let some of the smaller issues in his life squeak by ("Pap always said: The sweetest melon in the world is a snitched one"), while thinking about the big ones (helping his friend, Jim, an escaped slave).

At the time the story was taking place, slavery was legal. Helping an escaped slave was not. And yet the young Huck takes a stand. Damn. I'm going to have to re-read Huck Finn.

Well, anyway, if Mark Twain could take on a subject that divided a nation, then J.K. Rowling can take on a school for the... oh, let's call them 'metaphysically gifted'... sort of a Juilliard for telekinetics. [grin]

Okay, now that I've pretty much expressed my undying respect for Rowling and Mark Twain, let's get to the news, hints, tips and info available from the UseNet.

From the comp.sys.atari.st NewsGroup

'Coda' posts this tidbit about his USB Mouse Driver:

"I have decided to make the latest version of my USB mouse driver available for public download. This is considered an ALPHA release. There are things to fix, things to add etc, but it is usable and works on ST/TT/Falcon with EtherNat or NetUSBee, in TOS and MiNT. As for MagiC, you'll have to try it, I don't own it, so I can't develop for it.

Get it from the downloads page on http://www.janthomas.org.uk/ and don't forget to read the text file before you install it!

Obviously, if you don't have an EtherNAT (http://nature.atari.org) or a NetUSBee (http://hardware.atari.org) there's no point in downloading it!

Please let me know if you are using it (via the email address on my website, NOT the gmail spamtrap address I use for usenet).

Many thanks for your patience and for being unwilling ALPHA testers!

Version 0.90 is out.

Some things fixed. Some things added.

http://www.janthomas.org.uk/"

'Jao' asks for help in finding drivers:

"Does anyone know where I can find drivers for a Forget Me Clock II?

Actually I have the original drivers, but they no longer work (dates seem to be up to 1999 only). I'm wondering if there are any patches available?"

Greg Goodwin tells Jao:

"Here's a post from Aly from Sept. of last year:

'The problem with th FMCII software is that it won't go past the year 1999. The hardware RTC is fine, just that the software can't set it.

SOLUTION:
Edit the file FMCII.PRG with a hex editor. Find the first two occurrences of 63h Change these to 6Eh. And save.

Your FMCII.PRG program can now set dates up to 2010. 2006 is 106 in the FMC software.' "

Aly jumps in and adds:

"The downloadable and modified software is on atari-forum :-)

http://tinyurl.com/35k39u
[URL modified by Editor from:
www.atari-forum.com/wiki/index.php/
Fixing_the_Forget-Me-Not_Clock_software
for the sake of convenience]

Our buddy Fred Horvat asks about MagiCMac 'Classic':

"Has anybody tried and successfully gotten MagiCMac for OS9 to run on a PowerMac in the Classic environment from under OSX? My issue is that I

just recently upgraded machines from a G4 Cube to a PowerMac Dual G5. The G5 does not boot natively into OS9. So from OSX I can start the Classic environment (OS9) and try MagiCMac but all I get is a white screen and the system appears to freeze. I never ran Classic on any of my G4 Macs before. If I wanted OS9 I'd just boot into it. Earlier this year I got MagiCMac 6.20 for my Cube and was trying to get MacStip running when I bought my PowerMac G5. Now I'd like to start back where I left off with MagiCMac for OS9 but can not seem to get it running on the G5. I did try some other OS9 apps like iCab and Internet Explorer for OS9 and they appear to run just fine so the Classic Environment seems to be loaded properly on the G5."

Fidel-Sebastian Hunrichse-Lara tells Fred:

"That's, as far as I know, just impossible...

How often must I still repeat myself? MacSTip as a part of MacTCP-Connect is a crude hack that runs only with Old World ROM machines! Your Cube simply isn't an Old World ROM machine and therefore MacSTip won't work on it - there's definitively just no way...

All Macs prior to the iMac use Old World ROM, while the iMac and all subsequent models are New World ROM machines. In common use, the "Old World" designation usually applies to the early generations of PCI-based "beige" Power Macs (and sometimes the very first NuBus-equipped models)."

Fred replies:

"My mistake I meant MacTCP-Connect I wanted to set up. I know what an Old World Machine is as I have a couple 8500-120, 9500MP, and a 9600-200 which any of them could then run Mac-Stip. How then did Bengy at http://www.magical-sides.de the old MagiC Support Site run MacTCP-Connect on a G3-333 iMac? That was not an Old World Machine?

Like my original post said I had just gotten MagiCMac for OS/9 and was trying to setup up the TCP/IP connection with the Mac OS and MagiC when I got a new machine so I never did actually get it working. It appears that on my new G5 it is not possible to run MagiC under the Classic Environment.

[It] Stinks but not really that big a deal as I have other Macs in my office that I can run OS9. I would have just preferred to have as much as possible running on my G5.

If MagiCMac for OSX has TCP capability then I may be willing to spend the money to purchase it."

'Mark' adds:

"I have heard that Magic Mac won't work with OS 9.2. But it may work with a version of OS 9 up till 9.2, like 9.0 to 9.1.x
Classic is always going to be 9.2"

'ProToS' steps up and offers this:

"Magicmac and MacSTip work nice on 9.2.2"

Derryck Croker tells Fred:

"Andreas Kromke mentioned that the only way that there would be a TCP/IP driver for MagiCMacX would be if someone wrote the necessary module.

I thought that there was a certain amount of shooting oneself in the foot, but let's face it, the Internet browsing experience on the Mac is much better!"

Guillaume Tello asks about the venerable SH205:

"I'd like to know what is the capacity of this Hard drive (20Mb?) and what technology is inside: SCSI? (Cause I'd like to change the drive with a greater one but keeping the DMA adapter)"

Jason Harmon tells Guillaume:

"I'm trying to do something similar to you now.

I have a MegaFile 60 with a dying drive mechanism. From what I understand the SH 205 is a MegaFile 20 and may be very similar to what I have. The mechanism in mine is a 5.25" 60MB RLL drive. From what I understand, the controller in this drive serves two functions. It converts ACSI to SCSI, and then connects SCSI to RLL. However, since this logic is internal, I don't know how feasible it would be to try to modify the board to be able to connect a SCSI drive to it.

I just got an ICD AdSCSI ST host adapter, and am planning on ripping the guts out of the case and installing the ICD board and a 4GB SCSI drive in the case."

'Captain Midnight' tells Jason and Guillaume:

"I built a my first HD with a 60MB Seagate RLL drive and Supra Host Adapter. The HA converts to SCSI. Then a card inside the case translates to the RLL drive. The card is actually the SCSI device. AFAIK the card was just miniaturized to where it could be put on the drive making it a SCSI device.

Connecting a HA directly to a SCSI drive(s) is all that's needed.

Don't think the Atari HA is a good idea , even if physically possible, but leave that to those more knowledgeable. The HA will need to support the new drive.

On my later SCSI drives just used 50 conductor ribbon cable, a 50 pin IDC connectors on the drive and 2(if needed) 50 pin IDC centronics connectors on the outside with a Link HA on one of them. A centronics connector could be run to the outside from the internal HA as well. Come to think of it, did do that with the Supra too before getting the Link. Then there's termination.

I've also got 135&230MB SyQuests, a Floptical, 2 CD-ROMs and a 540MB Quantum drive in an Atari ST 3.5" floppy case that can be chained. The

Quantum requires parity so can't be used with either of these HA, unfortunately. Also unfortunate that it's been a long time since playing with them."

Djordje Vukovic posts this about TeraDesk:

"Hello all;

Version 3.92 of TeraDesk open-source desktop for the 16-bit and 32-bit lines of Atari computers is available at:

http://solair.eunet.yu/~vdjole/teradesk.htm

This release brings a small change (just five lines of code) made to set TeraDesk in agreement with Didier Mequignon's PICDESK utility for displaying desktop background pictures. Recently, an inquiry from a user made me aware of the existence of PICDESK, and it turned out that TeraDesk was already pretty much compatible with it- the picture was displayed, but there were some bad redraws. Only small corrections were needed to fix that.

See the history file and/or the hypertext manual for more information (i.e. how to set TeraDesk to enable display of desktop background pictures).

By the way, it seems that there is a bug in PICDESK: if it is set (and configuration saved) to display a monochrome IMG picture, on the next startup it attempts to display a GEM picture instead- and so nothing happens until a picture file is manually reselected.

PICDESK is not needed if one is using MyAES; that AES has a capability to display desktop background pictures. Also, it seems that PICDESK does not work with XaAES (but is ok with Atari AESes, N.AES, Geneva and MagiC).

In TeraDesk 3.92 there are also some other small improvements and bug fixes. Have fun."

THEN Djordje posts:

"An error has been made in the compilation of this release and it will not work on some systems. Please do NOT download or use it until the error is fixed. Sorry for inconvenience."

Jao now asks about transferring files:

"In my quest to replace my dying MegaFile 60, I've put together a new hard drive system based on an ICD AdSCSI ST connected to a 4GB SCSI drive. I've got the new drive configured with the latest ICD SCSI drivers, a 16MB boot partition, and a whole bunch of 256MB data partitions.

The big question I have is on how I can transfer data between my old drive and my new one. Let's ignore for the moment all the bad sectors, etc on the old drive.

Is there a way to connect both the ICD AdSCSI and the megafile at the same time so that I can just copy files between the drives? I had

tried to daisy chain the MegaFile from the "out" port on the ICD adapter, but when I did that the system would not boot from either hard drive.

Any useful pointers would be appreciated."

Uwe Seimet tells Jao:

"It might work with another driver. HDDRIVER is prepared for handling SCSI and ACSI drives in a mixed setup if a Link-compatible adapter is present. Since this setup is unusual I have never extensively tested it, though. What I would expect to work is a Megafile drive directly connected to the ST, a Link adapter connected to the DMA OUT port of the Megafile drive, and a SCSI drive connected to the Link.
You can use the HDDRIVER demo version (http://www.seimet.de/hddriver_english.html) in order to check whether you can use HDDRIVER at all with your hardware setup. Running the ID-check should be sufficient. If both drives are recognized things look good and HDDRIVER should be able to properly access both drives."

Jao tells Uwe:

"I tried this out (booting from floppy and then loading the trial HDDRIVER from it).

Unfortunately, the behavior I got was rather random, with the system seeing only the AdSCSI and not the MegaFile. I tried both orders in the ACSI chain but in no case could I get the system to see both drives, although once it saw the MegaFile and not the AdSCSI.

I was wondering if there is some sort of "ACSI ID" that needs to be set to allow the computer to distinguish between multiple ACSI devices attached to the system. I certainly have not heard of this, and there are no jumpers on the AdSCSI board to allow this to be set.

I guess my only option may be to simply find a stack of 720K floppies and use some backup software to backup and restore that way."

’ggnkua’ tells Jason:

"I have a couple of suggestions before you start searching for your old disk boxes.

Firstly, if you have a PC with a SCSI card you can connect the disk there, make a disk image and then extract the files from it, or if you use linux you can mount the disk directly. A PCI SCSI card should be dirt cheap to get hold of if you don’t have one.

Also, another idea would be to make (or buy) a cross serial cable and use Ghostlink on window$ or do$ to transfer files from the old disk to your PC partition and then get them back from there for your new disk.

If you find any of these 2 ideas attractive then I could dig up some links for you. Hope this helps."

Jason replies:

"Thanks for the Ghostlink suggestion. While its a bit slow, it is certainly easy to use and seems to be doing what I need it to.

The problem with this method is that the old drive in the MegaFile is not SCSI. It is an RLL drive (the MegaFile has a ACSI->SCSI->RLL controller in it, so without some additional hardware there is no way to hook it up to my PC's SCSI card.

If there is some software than can easily transfer a whole hard drive over serial to a PC, that would be great."

Uwe gets back to Jason and tells him:

"You have to ensure that both drives use different IDs. There are jumpers somewhere on the Megafile board to change the ID, and there are also jumpers on your SCSI drive to set the ID.

The AdSCSI does not have jumpers since the settings must be changed on the drives, not on the adaptor."

Jason tells Uwe:

"Ok, I may have misunderstood how this worked. I believe the AdSCSI is fixed as ID 6, and my SCSI drive connected to it is ID 0.

I was under the (probably mistaken) impression that devices connected to a separate ACSI controller would be part of a separate SCSI chains and would not collide with those on a different controller (similar to having 2 SCSI cards in a PC and having different drives connected to each card).

However, I will make sure the jumpers on the MegaFile board aren't set to 0 or 6 and see what happens."

Derryck Croker gives Jason one or two tips:

"Check that you have different SCSI IDs.

Also you say you have a "bunch of partitions". TOS does has a limit (16?) on the number you can have IIRC."

Well folks, that's it for this time around. Tune in again next week, same time, same station, and be ready to listen to what they are saying when...

PEOPLE ARE TALKING

=~=~=~=

->In This Week's Gaming Section - Atari's "My Horse and Me"!

"""""""""""""""""""""""""""""""""

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

Saddle Up for 'My Horse and Me!'

Atari, Inc. announced that it will publish My Horse and Me, the complete horseback riding and equestrian lifestyle video game experience for PC, Wii and Nintendo DS. Boasting the first and only exclusive worldwide license from the world's foremost horse sports organization, the Federation Equestre Internationale FEI (International Equestrian Federation), My Horse and Me features a realistic and immersive video game representation of the world of equestrian sports and is being developed by W!Games for Wii and PC and by Mistic for the DS.

Delivering all the excitement and fun of the equestrian life, from sports and leisure riding to horse care, My Horse and Me is a unique gaming experience for anyone with an interest or passion for horses. The game features the most accurate horse models and animations yet realized in a video game, alongside a richly rewarding game play experience, all set against a beautiful backdrop of charming indoor and outdoor environments.

"We are looking forward to providing the horse-enthusiast community with a rich and authentic game that allows gamers to take care of and compete in a variety of challenges with their horse." said Emily Anadu, Senior Product Manager, Atari Inc. "The game's distinctive and charming depiction of these noble animals is sure to win the hearts of horse devotees."

My Horse and Me has a rich variety of game play modes and options to give players a deep and rewarding experience. The Championship mode lets the player take part in competitions at indoor and outdoor locations around the globe ranging from rustic stables and classical riding schools to world-class tournament locations. A series of fun mini-games offer a variety of game play experiences alongside rewarding horse care game play and extensive customization.

The first horse sports simulation game to launch for Wii, My Horse and Me on Wii and PC is the first title of its kind to offer both first and third person camera modes, putting riders right in the saddle and creating a perfect training tool for practicing disciplines that riders face in real life.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

OLPC Now Ready for Mass Production

First, the good news. The nonprofit organization One Laptop Per Child (OLPC) announced on Monday that it has authorized the start of mass-production of the XO laptop, a low-cost but powerful device designed to reduce world poverty by extending the reach of the Internet to the planet's most remote regions.

The first laptops should roll off the assembly line in October of this year. Known as the B4, the laptop is the result of an intense collaboration by a large number of high-tech businesses and organizations, including OLPC, AMD, Google, Intel, Red Hat, eBay, and the open-source community.

"Since the inception of the XO laptop more than two years ago," said Gustavo Arenas, AMD's corporate vice president for high-growth markets and innovations, "AMD has been committed to helping the One Laptop per Child program succeed. We are proud to serve as a technology partner to such a noble and life-affecting project. The B4 machine paves the way for a final XO laptop that will change the lives of millions of children."

The computer runs on an efficient Linux-based operating system called Sugar, and the newest model incorporates some technological innovations that might well make their way into the mainstream laptop market. One of these innovations is a screen that is easy on the eyes and is capable of being easily read in full sunlight.

Another innovation is enhanced durability for widely varying climates and conditions. OLPC maintains that the laptop will function perfectly well in the rain, during dust storms, or even sitting in a puddle after a downpour. The Wi-Fi antenna - part of the computer's mesh-networking capability that is designed to allow an entire village to share a single Internet connection - also helps protect the computer from falls of up to 5 feet.

In addition, OLPC's B4 has extremely green power requirements. When being used as an e-book, the B4 consumes less than 1 watt of power, and can run for up to 12 hours on its battery, which can be recharged by hooking it to a solar-powered, multicomputer charger in a school, or even by using a built-in pull cord.

And now the bad news - or at least, the not terribly surprising news. According to Reuters, the official News Agency of Nigeria (NAN) reported last Thursday that one of its reporters saw pornographic images on several OLPC laptops in Abuja.

Reuters quoted NAN as saying that "[e]fforts to promote learning with laptops in a primary school in Abuja have gone awry as the pupils freely browse adult sites with explicit sexual materials."

OLPC officials quickly announced that they would add filtering software to the B4 laptop configuration, but did not respond to queries about which filtering software would be added or who would be responsible for

determining the settings of the software.

Dell To Expand Linux PC Offerings

Dell Inc Windows, said the founder of a company that offers Linux support services.

Mark Shuttleworth, who created a version of Linux software named Ubuntu, said Dell is happy with the demand it has seen for Linux PCs that were introduced in May.

Dell, the world’s second-largest PC maker after Hewlett-Packard Co, now offers three consumer PCs that run Ubuntu Linux.

"What’s been announced to date is not the full extent of what we will see over the next couple of weeks and months," Shuttleworth said an interview late on Wednesday.

"There are additional offerings in the pipeline," he said. Shuttleworth founded Canonical Inc to provide support for Ubuntu Linux.

A Dell spokeswoman, Anne Camden, declined comment, saying the company does not discuss products in the pipeline.

She added that Dell was pleased with customer response to its Linux PCs. She said Dell believed the bulk of the machines were sold to open-source software enthusiasts, while some first-time Linux users have purchased them as well.

Open-source software refers to computer programs, generally available over the Internet at no cost, that users can download, modify and redistribute.

The Linux operating system is seen as the biggest threat to Microsoft’s Windows operating system.

Shuttleworth said sales of the three Dell Ubuntu PC models were on track to meet the sales projections of Dell and Canonical. He declined to elaborate.

Companies like his privately held Canonical Inc, Red Hat Inc make money by selling standardized versions of Linux programs and support contracts to service them.

There are dozens of versions of Linux, available for all sorts of computers from PCs to mainframes and tiny mobile devices.

Shuttleworth said his company was not in discussions with Hewlett-Packard or the other top five PC makers to introduce machines equipped with Ubuntu.

The other three top PC makers are Lenovo Group Ltd, Acer Inc and Toshiba Corp.

Nothing Sure But Death And The Internet Tax Debate

As a federal ban on discriminatory and access taxes on the Internet approaches a Nov. 1 expiration date, Congress is once again embroiled in a question that comes up every three or four years: To what degree does the Internet merit special federal protection from state and local tax collectors?

The tax moratorium, which does not affect the states right to tax e-commerce, was first passed in 1998 and was extended twice since then. While some senators have recently suggested they are not fully convinced it should be preserved, House members overseeing the issue agree that it should be, either temporarily or permanently.

"It sounds like just about everybody s in agreement that we ve got to extend the moratorium and perhaps make it permanent," said Rep. John Conyers, D-Mich., Thursday at a hearing of the House Judiciary Subcommittee on Commercial and Administrative Law.

Lawmakers agree that the very definition of Internet access needs to be refined because not all states have interpreted it the same way. It s clear today that states can t tax the provision of Internet connectivity, such as DSL and cable modem services. However, the ban s proponents want a broader definition to make it clear that the transport components of Internet connectivity (such as Internet backbone service) and services unrelated to access, such as e-mail and instant messaging, won t be taxed either.

The major telephone companies and cable providers are the key proponents of a permanent Internet access tax ban, and they are joined by IT companies, including Apple and Cisco, as well as Internet-based businesses, including Amazon.com, eBay and Yahoo. Collectively lobbying as the Don t Tax Our Web Coalition, these groups would bear the brunt of access taxes if the ban isn t preserved or if Congress doesn t make it clear that services unrelated to access aren t included in it. The cost of such taxes would be passed along to business and consumer end users.

The coalition is divided on the issue of Internet sales taxes, which will likely be addressed in separate legislation.

The states are pressing for a narrower definition of Internet access, fearing that if the definition is too broad they will be unable to tax traditional telecommunications and video services that are bundled with Internet access. VoIP was explicitly exempted when Congress last extended the ban, and the states are concerned that non-access related emerging services, such as IP TV, could end up tax-free if service providers bundle them with connectivity.

Two bills pending in the House would make the ban permanent, but questions have arisen whether the Internet is sufficiently mature to thrive without eternal federal protection. A pending Senate bill would extend the ban for another four years.

"Since 1998, [Internet-related business has] grown and in 2006 was deemed to be worth an estimated $108.7 billion," said Rep. Linda Sanchez, D-Calif., who chairs the subcommittee. "What was still seen as a novelty by some in 1998, has become a daily part of life at home, in school, and in the workplace."

The states support the Senate bill, arguing that Congress should not pass

a permanent ban on an unpredictable technology. The Senate bill also preserves an exemption for nine states that had Internet taxes in place in 1998. David Quam, director of Federal Relations at the National Governors Association, told lawmakers at Thursday s hearing that the House legislation would cost those states as much as $120 million in tax revenue a year.

School Conducts Anti-Phishing Research

The e-mail appeared to be a routine correspondence between two friends. "Check this out!" it read, then listed a Web address.

But the note was fake, part of an online ruse called phishing that has become a scammer’s favorite way to get sensitive information from unsuspecting computer users.

The catch? The scammers were Indiana University researchers, the e-mail an experiment.

"I didn’t know I was being used," said Kevin McGrath, 25, a doctoral student at Indiana University whose e-mail address was one of hundreds used as "passive participants" for an experiment to study who gets duped by phishing.

As universities nationwide study ways to protect online security, methods at Indiana are raising ethical and logistical questions for researchers elsewhere: Does one have to steal to understand stealing? Should study participants know they are being attacked as part of a study? Can controlled phishing ever mimic real life?

Indiana researchers say the best way to understand online security is to act like the bad guys.

"We don’t believe that you can go and ask people, ’Have you been phished?’ There’s a stigma associated with it. It’s like asking people, ’Have you been raped?’" said Markus Jakobsson, an associate professor of informatics who directs IU’s Anti-Phishing Group.

The university has conducted nearly a dozen experiments in the last two years. In one, called "Messin’ With Texas," researchers learned mothers’ maiden names for scores of people in Texas. Maiden names often are used as a security challenge question.

Another conducted in May found that 72 percent of more than 600 students tested on the Bloomington, Ind., campus fell for an e-mail from an account intended to look familiar that sought usernames and passwords.

By contrast, only 18 percent of 350 students in a separate control group were fooled when they received e-mails from addresses they did not recognize.

The experiments found that hackers have the most success by using hijacked Web addresses or e-mail accounts that look real. The research also showed computer users generally have little knowledge of Web site security certificates and leave themselves open to attack with poorly configured routers or operating systems.

Understanding those weaknesses is a key to combatting phishing, which accounted for nearly three-quarters of 11,342 online attacks recorded between January and March, according to the US-Cert, which monitors online attacks for the Department of Homeland Security.

Many companies have taken steps to protect consumers, but none have proven entirely effective; which is why IU believes it’s important to understand phishing "in the wild," as Jakobsson describes it.

Federal laws governing university research allow scientists to use deceptive means if the risk participants face is minimal and no greater than what they would face in daily life.

Peter Finn, who serves on the Indiana review board that approves the studies, said the university believes the phishing experiments fall within those guidelines; even though about 30 students complained about the methods.

"The probability of harm from the study is nowhere near the magnitude of the harm that would result from actual phishing attacks," Finn said.

Jakobsson said researchers take steps to protect information from hackers who might snoop on the studies. The fake Web sites and e-mails used in the phishing attempts are created behind a secure server. No information submitted by test subjects is stored. The experiments, which are not encrypted in order to mirror real conditions, record only that someone gave information; not what they provided.

Celia B. Fisher, a human research ethicist at Fordham University in New York, said the experiments qualify as "deception research" and are legal, even necessary.

"There is no way to find this information out without deceiving the participants, because as soon as you tell them what you’re doing, you won’t have any real information," she said.

But Lorrie Cranor, who directs an anti-phishing group at Carnegie Mellon in Pittsburgh, said controlled laboratory studies can be just as useful.

The school has developed an online tool accessible only from its labs called "Anti-Phishing Phil" to lead participants through scenarios based on actual phishing attempts. The experiment hopes to determine which methods work the best at deceiving users.

Cranor’s research has found that successful phishing attempts rely on human vulnerabilities such as greed, curiosity, ignorance and fear.

"When you talk to someone, you look in their eyes and say, "Does this look like they’re telling the truth?’ And we get pretty good at making these judgments," she said. "But most of are not very good at making these judgments online."

Conditioning users to recognize those weaknesses before it’s too late is the safest way to combat phishing, she said.

"If we were to collect personal information from people, we have to be very careful," Cranor said. "You don’t want to be responsible for holding a list of people’s Social Security numbers."

Lawsuit Seeks To Shut Down Facebook

The owners of a rival social networking Web site are trying to shut down Facebook.com, charging in a federal lawsuit that Facebook's founder stole their ideas while they were students at Harvard.

The three founders of ConnectU say Mark Zuckerberg agreed to finish computer code for their site, but repeatedly stalled and eventually created Facebook using their ideas.

The lawsuit's allegations against Zuckerberg include fraud, copyright infringement and misappropriation of trade secrets. It asks the court to shutter Facebook and give control of the company and its assets to ConnectU's founders.

Facebook has responded by asking a judge to dismiss the lawsuit. A hearing is scheduled for Wednesday in U.S. District Court in Boston.

Facebook started in 2004, a few months before ConnectU went online, and now has 31 million users, compared with about 70,000 users for ConnectU, based in Greenwich, Conn. Last year, Facebook turned down a $1 billion buyout offer from Yahoo Inc.

A spokeswoman for Palo Alto, Calif.-based Facebook declined to comment. But in court filings, Facebook's attorneys say ConnectU has no evidence for "broad-brush allegations" against Zuckerberg, and deny he pilfered his ideas for Facebook from his fellow Harvard students.

"Each of them had different interests and activities," they wrote. "Only one of them had an idea significant enough to build a great company. That one person was Mark Zuckerberg."

Facebook and ConnectU connect college students and others online. Both allow users to post profiles with pictures, biographies and other personal information and create extended networks of people at their schools or jobs or with similar interests.

ConnectU originally filed suit in 2004, but it was dismissed on a technicality and immediately refiled. The lawsuit claims that in December 2002, ConnectU founders Cameron and Tyler Winklevoss - who are brothers - and Divya Narenda began to develop a social networking site for the Harvard community called Harvard Connection.

In November 2003, the three asked Zuckerberg to complete software and database work on the site. They repeatedly asked him to finish before they graduated in June 2004, and Zuckerberg assured them he was working hard to complete it, the lawsuit says.

"Such statements were false and Zuckerberg never intended to provide the code and instead intended to breach his promise ... and intended to steal the idea for the Harvard Connection Web site, and in fact he did so," the suit alleges.

Zuckerberg launched Thefacebook.com in February 2004. ConnectU started its Web site in May of that year. By beating ConnectU to the market, Facebook gained a huge advantage, the lawsuit claims.

ConnectU's founders have written on their Web site about the "ups and

downs" of their company history, including a programmer "who stole our ideas to create a competing site."

"But we've been troopers," they wrote. "At first we were devastated and climbed into a bottle of Jack Daniels for a bit, but eventually emerged with a bad headache and renewed optimism. We weren't going to lie down and get walked over like this."

China, FBI Bust Software Counterfeiters

Chinese police have busted up two criminal organizations and seized pirated software worth half a billion dollars, the culmination of two years of work with the FBI, officials from both countries said Tuesday.

The gangs pirated Microsoft Corp. and Symantec Corp. software and sold it around the world, including in the United States, said Gao Feng, an official with China's Ministry of Public Security.

In a news conference from the southern Chinese city of Shenzhen, Gao said police arrested 25 people and seized property worth about $8 million. Chinese police also confiscated counterfeit software with an estimated retail value of $500 million, according to an FBI statement.

Gao said Chinese police discovered in 2005 that the Chinese gangs were colluding with suspects in the United States and notified the FBI's Beijing office.

China has long been the world's leading source of illegally copied goods, including designer clothes, movies and music. The country has been under pressure to crack down, and that has been increasing ahead of next year's Summer Olympics in Beijing.

The Business Software Alliance, a trade group that tracks piracy, said in a statement Tuesday that software counterfeiting in China has dropped in recent years. But the group claims that global piracy took a $40 billion bite out of worldwide software revenue in 2006.

According to the FBI, Chinese police arrested Ma KePei and 10 others in Shanghai. Ma was indicted in 2003 in a New York court for making and distributing counterfeit Microsoft programs, but fled to China - where he is now accused of making fake Symantec security software.

In Shenzhen, a boomtown just over the border from Hong Kong, 14 people were arrested for making fake Microsoft programs, including Windows Vista and Office 2007. Six manufacturing and retail facilities were shut down, the FBI said.

"The majority of Chinese-based distributors advertised their products aggressively and recruited distributors via the Internet," the bureau said. Suspects were in custody and have been charged with copyright violations.

In related actions in Los Angeles, FBI agents seized about $2 million in counterfeit software from the Chinese groups.

Bonnie MacNaughton, a senior attorney on Microsoft's worldwide anti-piracy team, said the Shenzhen group was the "largest criminal

syndicate in Microsoft’s history," responsible for an estimated $2 billion in fake software sales.

"We believe that these arrests and the seizures associated with them will have significant impact on the distribution of high-quality counterfeit software," MacNaughton said in a phone interview.

Microsoft provided investigators with information gathered from customers and partners. The company’s 2-year-old Windows Genuine Advantage program, which scans computers for counterfeit programs, has substantially increased the number of piracy leads, MacNaughton said.

MacNaughton would not directly say whether piracy remained a problem in China, and instead noted that "we have a long way to go before we have all of our customers using genuine software."

New DIY Trojan Tool on Sale on the Internet

A new kit for building and customizing Trojan malware has been discovered for sale on the Internet.

With the appropriate name ’Pinch,’ the tool lets criminals with little technical knowledge specify a number of parameters such as which type of password to steal from infected machines. Alternatively, the tabbed-based interface can be made to turn the program into a straightforward key-logger set to capture all keystrokes, take screenshots, or steal specific file types.

Most disturbing of all, the program can also be configured so that infected systems are simply turned into proxies or bots to carry out malicious activity on remote computers, including downloading and hosting other malware. In addition, it can be hidden from the infected PC’s owner by opening unusual ports through which to communicate, or invoking rootkit-like self-protection.

"Pinch’s main danger is that it is very easy to use, so any malicious user with basic computer knowledge could create a Trojan in a very short time for very little money," explains Luis Corrons, technical director of PandaLabs, the company that has publicized the program.

The program is sophisticated enough to attack a named list of anti-virus engines, interfere with Windows firewall settings, and spread using a variety of means, including operating as a mass-mailing worm.

Its origins are unclear, but judging by the screenshots in PandaLabs’ analysis of the software, it is most likely Russian.

Malware kits are becoming one of the year’s big stories even if their origins lie further back in time.

Earlier this year, a DIY program for man-in-the-middle phishing was found doing the rounds on the wrong Web sites. It is certainly noteworthy that there are now a small but growing band of programs designed to automate the often complex programming behind malware for the non-programming criminal.

Government Warns Public On Fake E-mails

The federal agency charged with protecting consumers from Internet scams now finds itself wrapped up in one.

Identity thieves have sent thousands of bogus e-mails purporting to be from the Federal Trade Commission - as well as the Internal Revenue Service and Justice Department - in an attempt to trick consumers into divulging personal financial information.

The agencies are the latest institutions to be exploited in "phishing" scams, long the bane of large banks and credit card issuers.

Analysts who track online crime say that while financial institutions are still the most commonly hijacked brands, the use of federal agencies in the hoaxes is increasing and reflects criminals' desire to take advantage of the familiarity and authority of various government departments.

Phishing typically involves sending fraudulent e-mails that include links that direct recipients to fake Web sites where they are asked to input sensitive data. Phishers may also include attachments that, when clicked, secretly install "spyware" that can capture personal information and send it to third parties over the Internet.

Criminal gangs in the United States and overseas use the information to steal thousands of dollars from consumers or to sell their identities in what experts describe as a sophisticated underground economy surrounding identity theft.

The FTC said in June that corporate and banking executives, among other consumers, have received fake e-mails with spyware attachments purporting to be from the agency.

The Treasury Department, meanwhile, said June 27 it has received over 23,000 complaints about IRS-related phishing scams since an investigative arm of the department began tracking them in November 2005.

The scams have been "unprecedented both in terms of sophistication and the volume of reports we have received," J. Russell George, Treasury Inspector General for Tax Administration, said in a written statement.

Michelle Lamishaw, an IRS spokeswoman, said most of the hoax e-mails tell recipients they are under investigation or that they have a tax refund pending. Some are more sophisticated, including those targeted to small businesses that mention obscure agencies known primarily to business men and women such as the California Franchise Tax Board.

But government officials said recipients of such e-mails should be suspicious of their origin for one simple reason: federal agencies rarely communicate with citizens over e-mail.

Lois Greisman, associate director of the FTC's division of marketing practices, said, "We are the agency that brought you the Do Not Call Registry and CAN-SPAM," she said, referring to a 2003 law restricting commercial spam. "We're not likely to send out unsolicited e-mails."

Peter Cassidy, a spokesman for the Anti-Phishing Working Group, said

phishing first surfaced early this decade and took off in 2003. The APWG is a consortium of corporations, banks, software providers and law enforcement agencies whose members include eBay Inc., Microsoft Corp. and Yahoo Inc.

The scams are still growing rapidly: the number of phishing Web sites jumped to 37,438 in May, the APWG said in a report released July 8, more than triple the 11,976 reported in May 2006.

Phishing can carry significant economic costs for the victims and rewards for the perpetrators. Jeff Fox, technology editor at Consumer Reports, said that last September his group estimated consumers had lost $630 million to phishing scams in the previous two years.

A recent report from the Government Accountability Office, Congress’s investigative arm, put the figure at $1 billion annually.

Despite efforts to educate the public about the dangers of clicking on unknown links and attachments in spam e-mail, many computer users still do so.

Consumer Reports estimates that 8.2 percent of online households have submitted personal information in response to fraudulent e-mails in the past two years, Fox said. "It’s astounding," he added.

An entire underground economy has developed around identity theft, Cassidy said, with some groups specializing in sending fraudulent spam, while others act as brokers for stolen personal information. Both may be hired by organized crime groups that steal and launder money.

The rise of well-organized, financially motivated computer hackers is one of the biggest changes in online crime in the past ten years, said Dave Marcus, a research manager at security software maker McAfee Inc.

They have effectively replaced the stereotypical computer geek who seeks notoriety by creating the latest, nastiest computer virus, he said.

On the Net:

http://onguardonline.gov/index.html

Test Your Knowledge Of Online Scams

Think you’re smart at recognizing online scams?

Take a quiz to find out.

McAfee Inc.’s SiteAdvisor service has created a 10-question test to see whether you can spot "phishing" attempts to steal passwords and other personal information by mimicking popular Web sites such as eBay Inc.’s PayPal and News Corp.’s MySpace.

In eight questions, you are presented with two Web sites or e-mail messages and are asked to identify the authentic one. The final two questions test your general knowledge about scams.

Afterward, the McAfee site presents telltale signs to look for, such as

misspellings and suspicious Web addresses.

You can also download a tool that can help warn of sites known or suspected to be phishing scams. SiteAdvisor researchers also identify sites that produce spyware, viruses, excessive pop-up ads, junk e-mail or other threats.

Visit http://tinyurl.com/ytec4u to take the quiz.

MySpace Deletes 29,000 Sex Offenders

Popular Internet social network MySpace said on Tuesday it detected and deleted 29,000 convicted sex offenders on its service, more than four times the figure it had initially reported.

The company, owned by media conglomerate News Corp, said in May it had deleted about 7,000 user profiles that belonged to convicted offenders. MySpace attracts about 60 million unique visitors monthly in the United States.

The new information was first revealed by U.S. state authorities after MySpace turned over information on convicted sex offenders it had removed from the service.

"The exploding epidemic of sex offender profiles on MySpace - 29,000 and counting - screams for action," Connecticut Attorney General Richard Blumenthal said in a statement.

Blumenthal, who led a coalition of state authorities to lobby MySpace for more stringent safeguards for minors, and other state AGs have demanded the service begin verifying a user’s age and require parental permission for minors.

The minimum age to register on MySpace is 14.

"We’re pleased that we’ve successfully identified and removed registered sex offenders from our site and hope that other social networking sites follow our lead," MySpace Chief Security Officer Hemanshu Nigam said in a statement.

The service has come under attack over the past year after some of its young members fell prey to adult predators posing as minors. The families of several teenage girls sexually assaulted by MySpace members sued the service in January for failing to safeguard its young members.

Late last year, it struck a partnership with background verification company Sentinel Tech Holdings Corp. to co-develop the first U.S. national database of convicted sex offenders to make it easier to track offenders on the Internet.

Convicted sex offenders are required by law to register their contact information with local authorities. But the information has only been available on regional databases, making nationwide searches difficult.

As of May, there were about 600,000 registered sex offenders in the United States.

You’re Not the Only One Reading Your E-Mail

Do you know who is reading your e-mail?

Has the fact that there is a good chance that your place of work is reading your outbound e-mail, even those that you send from your personal Web mail accounts, changed your behavior?

Did you know that more than one-quarter of U.S. companies have fired an employee in the last year for violating e-mail policies?

If your answer to all three of the above questions was "no," you might breathe a sigh of relief to learn that your answers put you squarely in the majority of U.S. employees. But the relief will last only until the implications of these answers set in. The odds are, someone else in your company knows you’re reading this article right now.

Nearly one-third (32 percent) of large U.S. companies employ staff to read or otherwise analyze outbound e-mail, and this amount grew to 39 percent among companies with more than 20,000 employees.

This was among the findings of the 2007 Outbound E-Mail and Content Security in Today’s Enterprise study conducted by Forrester Research and released July 23 by Proofpoint, an e-mail security firm based in Cupertino.

Not only are companies reading outbound e-mail, they’re employing individuals whole sole purpose is to sift through the contents of an employee’s computer. More than one in six of the companies surveyed employed staff whose primary or exclusive job function was to monitor e-mail content. This number jumped to nearly one-fifth (19.4 percent) among companies with more than 20,000 employees.

Who are the paid snoops at large organizations? Is "E-Mail Eavesdropper" a new job title?

"There are a multitude of people within an enterprise that may have this role, from the e-mail administrator to compliance folks who are responsible for making sure that e-mail isn’t violating any internal policies," Keith Crosley, director of market development at Proofpoint told eWEEK.

While this level of peering over an employee’s shoulder may seem excessive, the companies in question are not likely to agree. They estimated that nearly one in five outgoing e-mails (18.9 percent) contained content that posed a legal, financial or regulatory risk. The most common form of non-compliant content was e-mail that contained confidential or proprietary information.

Companies weren’t found to be sitting idly by when they learned of a potential leak. More than one in three (33.8 percent) organizations surveyed had investigated a suspected e-mail leak of confidential or proprietary information in the last 12 months. Just shy of one-third (31.8 percent) had investigated a possible violation of privacy or data protection in the same time frame.

Furthermore, more than one quarter of companies (27.6 percent) had

terminated an employee for violating e-mail policies in the last year, and nearly half (45.5 percent) had disciplined one.

Read more here about MessageLabs managed e-mail service that lets enterprises control content sent to and from employees.

Of all violations that companies monitored for, offensive content that did not threaten an organization’s security was the least of their concerns.

"While companies are concerned about all of these things, offensive content consistently comes in at the bottom of these concerns. For all companies, 57 percent said they were concerned about monitoring e-mail for offensive content," said Crosley.

Despite cracking down on employees who were putting confidential information at risk, a surprising number of companies had no published e-mail policy whatsoever, though the number had declined since 2004, the first year the survey was conducted.

"One thing that was really good to see was we saw the biggest adoption of acceptable use policies this year of all the years we’ve done this survey. But, I was still surprised to see that 11 percent still did not have a formal mail use policy," said Crosley.

In addition to e-mail policies, the wide variety of opportunities to share information with Web 2.0 and social media software signaled a need for policies with a greater reach.

"Organizations really need to have well thought out and clearly articulated policies on media and information sharing, from YouTube to blogs, e-mail and message boards," said Crosley.

Though the majority of organizations surveyed (59.4 percent) had conducted a formal training on e-mail security policies in the last 12 months, a significant amount had not.

"Policies aren’t any good unless employees know what they are. You need to articulate it and educate them," said Crosley.

"You want to be able to consistently apply these kinds of actions and be clear about what you allow and what you don’t allow; what you want to protect and what is public. The point is not to get people in trouble, [but] to protect digital data and comply with regulations," said Crosley.

Wasting Time At Work? You’re Not Alone

Americans who feel bored and underpaid do work hard - at surfing the Internet and catching up on gossip, according to a survey that found U.S. workers waste about 20 percent of their working day.

An online survey of 2,057 employees by online compensation company Salary.com found about six in every 10 workers admit to wasting time at work with the average employee wasting 1.7 hours of a typical 8.5 hour working day.

Personal Internet use topped the list as the leading time-wasting

activity according to 34 percent of respondents, with 20.3 percent then listing socializing with co-workers and 17 percent conducting personal business as taking up time.

The reasons why people wasted time were varied with nearly 18 percent of respondents questioned by e-mail in June and July said boredom and not having enough to do was the main reason.

The second most popular reason for wasting time was having too long hours (13.9 percent), being underpaid (11.8 percent), and a lack of challenging work (11.1 percent).

"While a certain amount of wasted time is built into company salary structures, our research indicates that companies with a challenged and engaged workforce can expect more productivity in return," said Bill Coleman, chief compensation officer at Salary.com.

While the amount of time wasted at work seems high, Coleman said the numbers have improved, with the amount of time wasted dropping 19 percent since Salary.com conducted its first annual survey on slacking at work in 2005. Then workers reported wasting 2.09 hours of their working day.

"I think (the decline) is really a result of the economy and that there’s more business, more work available and less time to sit around wondering what you are going to do with your day," Coleman told Reuters.

Wasting Time Online Could Be A Thing Of The Past

Does your company monitor how much time you spend on YouTube and eBay? Perhaps it should.

Employees waste more than 81 minutes of work time in personal computer activity on average and 13% squander more than two hours a day on recreational computer activities, according to an old AOL/Salary.com survey.

And, those considered top employees can be the worst offenders.

To minimize all that time lost, software provider Ascentive has launched a "workplace activity management" application called BeAware Corporate Edition. The software aims to help increase employee productivity, cut down on wasted time, and protect company data.

A remote set-up option allows employers to install the software to each employee and track all employee PC activity with live, real-time monitoring of emails, web surfing, chat and program use. Individuals, departments, and the enterprise can view resulting reports.

The system can also notify individuals and groups when a user accesses specific words, Web sites or applications. Ascent offers a stealth mode it says makes the program undetectable.

The software can track employees as they work in the field, at other company offices or on the road. It offers a personal time feature that allows employees to take care of personal business during lunch and other approved breaks. Ascent promises privacy during those times and allows pop-up windows to tell employees how much personal time they have for

computer use.

Ascentive President Adam Schran said BeAware can help reward employees for great behavior.

"It’s now easier, almost effortless, for bosses to help make their companies more efficient and effective," he said, adding that software has little (1%) impact on network speeds.

It can be deployed to 10,000 employees. The application goes for $89.95 per computer, with discounted rates for five computers or more.

"Our clients have told us that they see unwanted Internet usage by their employees drop as much as 90% almost immediately after BeAware is installed," Schran said in a prepared statement.

Then again, there is always the water cooler.

Young Keep It Simple In High-Tech World

While young people embrace the Web with real or virtual friends and their cell phone is never far away, relatively few like technology and those that do tend to be in Brazil, India and China, according to a survey.

Only a handful think of technology as a concept, and just 16 percent use terms like "social networking," said two combined surveys covering 8- to 24-year-olds published on Tuesday by Microsoft and Viacom units MTV Networks and Nickelodeon.

"Young people don’t see "tech" as a separate entity - it’s an organic part of their lives," said Andrew Davidson, vice president of MTV’s VBS International Insight unit.

"Talking to them about the role of technology in their lifestyle would be like talking to kids in the 1980s about the role the park swing or the telephone played in their social lives - it’s invisible."

The surveys involved 18,000 young people in 16 countries including the UK, U.S., China, Japan, Canada and Mexico.

Terms most frequently used by the young when talking about technology related to accessing content for free, notably "download and "burn."

The surveyors found the average Chinese computer user has 37 online friends they have never met, Indian youth are most likely to see cell phones as a status symbol, while one-in-three UK and U.S. teenagers say they cannot live without games consoles.

"The way each technology is adopted and adapted throughout the world depends as much on local cultural and social factors as on the technology itself," said Davidson.

For example, the key digital device for Japan’s young is the cell phone because of the privacy and portability it offers those who live in small homes with limited privacy.

They found Japanese children aged eight to 14 have only one online

friend they have not met, compared to a global average of five. Some 93 percent of Chinese computer users aged 8-14 have more than one friend online they have never met.

Davidson said this was encouraging those aged 8-14 in China to select online over television - a trend not seen in any other market in that age group.

The changes in how the youth market engages with technology is keenly followed by advertisers and content firms.

"Traditional youth marketing considered opinion formers and influencers to be a small elite, but these days the elite has become much larger," said Davidson.

For parents worried about what their children are getting up to amid the wave of gadgets, little has changed in a generation.

The surveyors found the most popular activities the under-14s enjoy were
watching TV, listening to music and being with friends. The rankings for those older was similar although listening to music was top.

Man Burns Down Trailer In Online Feud

A Navy man who got mad when someone mocked him as a "nerd" over the Internet climbed into his car and drove 1,300 miles from Virginia to Texas to teach the other guy a lesson.

As he made his way toward Texas, Fire Controlman 2nd Class Petty Officer Russell Tavares posted photos online showing the welcome signs at several states' borders, as if to prove to his Internet friends that he meant business.

When he finally arrived, Tavares burned the guy's trailer down.

This week, Tavares, 27, was sentenced to seven years in prison after pleading no contest to arson and admitting he set the blaze.

"I didn't think anybody was stupid enough to try to kill anybody over an Internet fight," said John G. Anderson, 59, who suffered smoke inhalation while trying to put out the 2005 blaze that caused $50,000 in damage to his trailer and computer equipment.

The feud started when Anderson, who runs a haunted house near Waco, joined a picture-sharing Web site and posted his artwork and political views. After he blocked some people from his page because of insults and foul language, they retaliated by making obscene digitally altered pictures of him, he said.

Anderson, who went by the screen name "Johnny Darkness," traded barbs with Tavares, aka "PyroDice."

Investigators say Tavares boiled over when Anderson called him a nerd and posted a digitally altered photo making Tavares look like a skinny boy in high-water pants, holding a gun and a laptop under a "Revenge of the Nerds" sign.

Tavares obtained Anderson’s real name and hometown from Anderson’s Web page about his Museum of Horrors Haunted House.

Tavares took leave from his post as a weapons systems operator at the AEGIS Training and Readiness Center in Dahlgren, Va., and started driving. Investigators say he told them he planned to point a shotgun at Anderson and shoot his computer.

Instead, when he got to Elm Mott - after posting one last photo of a "Welcome to Texas" sign - Tavares threw a piece of gasoline-soaked plastic foam into the back of Anderson’s mobile home and lit a flare, authorities say.

Tavares’ attorney, Susan Kelly Johnston, said his trip to the Waco area was a last-minute decision during a cross-country trip to visit his parents in Arizona. She said he never intended to hurt Anderson and did not think he was in the trailer when he set the fire.

James Pack, an investigator with the McLennan County Sheriff’s Office, caught up with Tavares after talking to people in several states and Spain who had been involved in the online feud. Tavares’ cell phone records showed he was in the Waco area at the time of the fire, Pack said.

Tavares told investigators that Anderson had spread computer viruses and insulted his online friends for too long, Pack said.

"He lost everything - all over an Internet squabble," the investigator said.

Tavares was discharged last year from the Navy, where he earned several medals - including the pistol expert and rifle expert medals - in his nine-year career, said Navy spokesman Mike McLellan.

Tavares would not let the feud go even at his sentencing. According to Pack, Tavares took cell-phone photos of Anderson in the courtroom while the judge was hearing another case. Authorities ordered the photos erased.

Anderson, an ex-Marine who served in Vietnam, said he continues to be harassed online, has been startled by people knocking on his window late at night and found bullet holes in a door to his business.

He said he is convinced the harassment is related to the Internet feud and plans to spend $30,000 on more fencing topped with barbed wire.

"Before this happened, the rule was: Nobody messes with the haunted house guy," Anderson said.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for

profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.